

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number  
**WO 02/07456 A1**

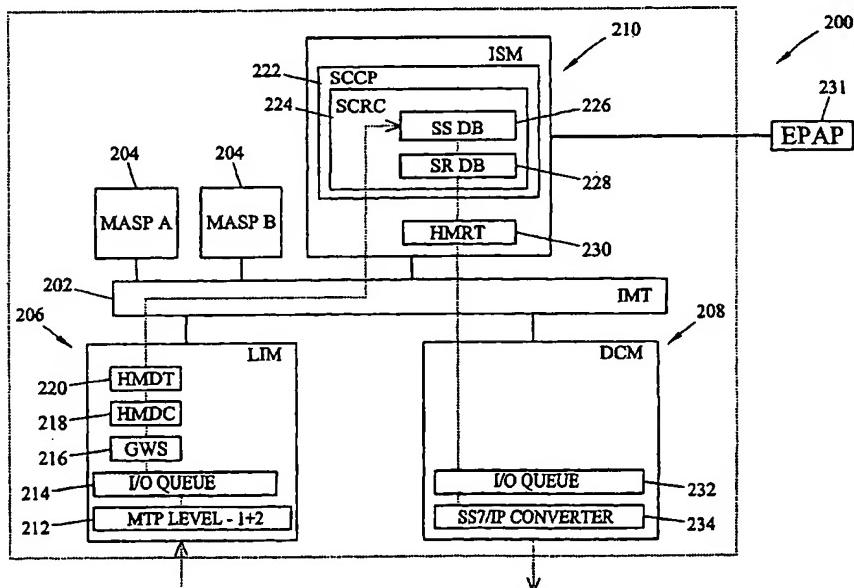
- (51) International Patent Classification<sup>7</sup>: H04Q 3/00, H04M 7/00, 3/436
- (21) International Application Number: PCT/US01/22093
- (22) International Filing Date: 13 July 2001 (13.07.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
60/218,204 14 July 2000 (14.07.2000) US
- (71) Applicant (*for all designated States except US*): TEK-ELEC [US/US]; 26580 West Agoura Road, Calabasas, CA 91302 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): CHANG, James, Tjin-Tek [US/US]; 102 Harrison Court, Chapel Hill, NC 27516 (US). MCCANN, Thomas, Matthew [US/US]; 117 Oxyard Way, Morrisville, NC 27560 (US). MARSICO, Peter, J. [US/US]; 201 Westbrook Drive, #D15,
- Carrboro, NC 27510 (US). HALEY, Allen, Woodward, Jr. [US/US]; 903 Parkwood Court, McKinney, TX 75070 (US). RUSHNAK, Linda, Ann [US/US]; 3540 Kimble Drive, Plano, TX 75025-4443 (US).
- (74) Agent: JENKINS, Richard, E.; Jenkins & Wilson, P.A., University Tower, Suite 1400, 3100 Tower Boulevard, Durham, NC 27707 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: TRIGGERLESS SCREENING SERVICES



**WO 02/07456 A1**



(57) **Abstract:** Method and systems for providing triggerless screening services include a triggerless screening service routing node and a message processing platform. The triggerless screening service routing node identifies call setup messages that require one or more call screening services and diverts the messages to a message processing platform. The message processing platform performs at least one screening action on the call setup message and modifies the messages to include the type and result of the screening action.



**Published:**

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## TRIGGERLESS SCREENING SERVICES

5

Priority Application Information

This application claims the benefit of United States Provisional Patent Application Number 60/218,204 filed July 14, 2000, the disclosure of which is incorporated herein by reference in its entirety.

10

Technical Field

The present invention relates generally to triggerless intelligent network screening services. More particularly, the present invention relates to methods and systems for providing triggerless intelligent network screening services based on call setup messages, such as ISDN user part (ISUP) messages or session initiation protocol (SIP) messages.

Background Art

The intelligent network (IN) and advanced intelligent network (AIN) were designed to provide additional services to telecommunications network subscribers. Examples of IN and AIN service include 800 number service, calling card verification service, line information database service, etc. Both the AIN and IN architecture moved the databases required to provide these services from the end office switching systems to database nodes, which are referred to in the SS7 network as service control points or SCPs.

Moving IN/AIN service databases to SCPs simplified switching system architecture and allowed services to be modified or updated at the SCPs without modification of each end office switching system served by the SCPs. However, triggers, usually implemented in software, were required to be set at each SSP in order to access IN/AIN services. For example, if a particular subscriber wished to access an AIN service, a trigger would be required to be manually set at the end office serving that subscriber in order

-2-

to allow the subscriber to access the service. Requiring triggers to be set at end offices places a heavy burden on switching system operators, since these triggers must be provisioned for each subscriber and each service at each end office.

- 5 Another problem with providing trigger-based services is that they require database queries, which increase network traffic and call setup time. For example, when a subscriber initiates a call, and that party's end office detects that IN/AIN service is required, the end office launches a transaction capabilities application part (TCAP) query to an SCP. A signal transfer point  
10 receives the TCAP query, and routes the TCAP query to the SCP. The SCP formulates a TCAP response and forwards the response back to the end office through the STP. From the time that the query is launched until the response is received, call processing is suspended at the end office, which increases call setup time. In addition, the TCAP query and response  
15 messages increase network traffic.

In order to alleviate the problem associated with triggered network services, some triggerless network services have been developed. For example, commonly-assigned, co-pending international patent publication number WO 00/60839, published October 12, 2000, discusses a triggerless  
20 number portability solution in which a signal transfer point performs number portability database lookups based on call setup messages received from end offices without requiring triggers at the end offices. While this solution greatly reduces the time required for number portability lookups, there still exists a need for providing other types of triggerless IN-services, such as  
25 screening services. As used herein, the phrase "screening services" includes services based on screening one or more parameters in a call setup message. Examples of such screening services include calling number screening, point code screening, credit limit screening, and a variety of other screening services. These screening services have either not been  
30 previously provided or have been provided only using triggers or end-office-based network implementations.

-3-

In connection with providing triggerless call screening services, there is currently no standard method for notifying a calling or called party end office or other node of the result of a screening action. Unless a screening action is performed by a particular end office, that end office may not know 5 of the result of a screening action that occurred elsewhere in the network. Information regarding the results of a screening action can be important, for example, for notifying a called or calling party of the result of the screening action or for redirecting a call to another location. Accordingly, there exists a long-felt need for methods and systems for communicating call screening 10 results to end offices or other nodes that did not perform the screening action.

Disclosure of the Invention

According to one aspect, the present invention includes a triggerless 15 screening service screening routing node and a message processing platform for screening call setup messages and communicating call screening information to a receiving end office without requiring end office triggers to invoke screening actions. The triggerless screening service routing node identifies messages that require call screening processing and 20 redirects the messages to a message processing platform. The message processing platform performs one or more call screening operations based on the received call setup messages, modifies the messages to include information to indicate to the results of the call screening action, and forwards the messages to their destinations.

25 Accordingly, it is an object of the present invention to provide a system and method of providing IN service in a communications network without the need for explicit IN triggers or query messages.

It is another object of the invention to provide a method and system 30 for communicating the results of a call screening action to an end office or other node that did not perform the call screening action.

-4-

Some of the objects of the invention having been stated hereinabove, other objects will be evident as the description proceeds, when taken in connection with the accompanying drawings as best described hereinbelow.

5

Brief Description of the Drawings

Figure 1 is a block diagram of an internal architecture of a conventional signaling gateway containing exemplary hardware suitable for use with a triggerless screening service routing node according to embodiments of the present invention.

10

Figure 2 is a block diagram of an internal architecture of a triggerless screening service routing node according to an embodiment of the present invention.

15

Figure 3 is a block diagram illustrating an SCCP-encapsulated ISUP signaling message generated by a triggerless screening service routing node according to an embodiment of the present invention.

Figure 4 is a block diagram of an internal architecture of an IN message processing platform (MPP) node according to an embodiment of the present invention.

20

Figures 5A and 5B are flow charts illustrating processing of a received ISUP message by a triggerless screening service routing node according to an embodiment of the present invention.

Figure 6 is a flow chart illustrating IN screening service processing of an ISUP message by an IN MPP node according to an embodiment of the present invention.

25

Figure 7 is a network diagram illustrating signaling message flow associated with the operation of a triggerless IN screening system according to an embodiment of the present invention.

30

Figure 8 is a network diagram illustrating signaling message flow associated with a triggerless IN screening system according to an alternate embodiment of the present invention.

Detailed Description of the Invention

According to one embodiment, the present invention includes a triggerless screening service routing node and a message processing platform for screening call setup messages and communicating call screening information to a destination node. The triggerless screening service routing node and the message processing platform are described and illustrated herein as collections of modules and databases. It is understood that these modules and databases may be implemented in software residing in memory and executed by one or more general-purpose microprocessors. Alternatively, the modules and databases described herein may be implemented in hardware, such as application-specific integrated circuits (ASICs). Any combination of hardware, software, or hardware and software for providing triggerless IN screening functionality as described herein is intended to be within the scope of the invention.

15       Exemplary Hardware Platform for Triggerless Screening ServiceRouting Node

A triggerless screening service routing node according to an embodiment of the present invention utilize an underlying hardware configuration similar to that of a conventional signal transfer point or SS7/IP gateway. Exemplary commercially-available hardware platforms suitable for use with embodiments of the present invention include the Eagle® signal transfer point or the IP<sup>TM</sup> Secure Gateway, both available from Tekelec of Calabasas, California. Figure 1 illustrates an exemplary internal architecture of an SS7/IP gateway suitable for use with a triggerless screening service routing node according to an embodiment of the present invention. In Figure 1, an SS7/IP gateway 100 includes the following subsystems: a maintenance and administration subsystem (MAS) 102, a communication subsystem 104 and an application subsystem 106. MAS 102 provides maintenance communications, initial program loading, peripheral services, alarm processing and system disks. Communication subsystem 104 includes an interprocessor message transport (IMT) bus that is the main communication

-6-

bus among all subsystems in gateway 100. The IMT bus includes 125 Mbps counter-rotating serial buses.

Application subsystem 106 includes application cards or printed circuit boards capable of communicating with the other cards through the IMT bus.

- 5 Numerous types of application cards can be included in gateway 100. Exemplary application cards include a link interface module (LIM) 108 that provides SS7 links and X.25 links, a data communication module (DCM) 110 that provides a TCP/IP interface to external nodes, and an application service module (ASM) 112 that provides global title translation and other
- 10 services. A translation service module (TSM) 114 may also be provided to support triggered local number portability service. The functions of these modules relating to triggerless screening service processing will be described in detail below.

Exemplary Internal Architecture of Triggerless Screening Service Routing

- 15 Node

Figure 2 illustrates the internal architecture of a triggerless screening service routing node according to an embodiment of the present invention. In Figure 2, a triggerless screening service routing node 200 includes a high speed interprocessor message transport communications bus 202. A number of distributed processing modules or cards are coupled to IMT bus 202, including: a pair of maintenance and administration subsystem processors 204, an SS7-capable link interface module 206, a TCP/IP-capable data communication module 208, and an ISDN user part service module (ISMS) 210. These modules are physically connected to the IMT bus 202 such that signaling and other types of messages may be routed internally between all active cards or modules. For simplicity of illustration, only a single LIM 206, a single DCM 208, and a single ISMS 210 are illustrated in Figure 2. However, in a distributed processing environment, multiple LIMs 206, DCMs 208, and ISMSs 210 may be included within 30 triggerless screening service routing node 200.

MASP pair 204 implement the maintenance and administration subsystem functions described above. As MASPS 204 are not particularly

relevant to a discussion of the triggerless screening processing attributes of the present invention, a detailed discussion of their function is not provided herein. MASPS are included for completeness purposes only.

LIM 206 includes a number of component processes including an SS7

- 5 MTP level 1 and 2 process 212, an I/O buffer or queue 214, a gateway screening (GWS) process 216, an SS7 MTP level 3 message handling and discrimination (HMDC) process 218, and a message handling and distribution (HMDT) process 220. MTP level 1 and 2 process 212 sends and receives digital data over a particular physical interface. MTP level 1 and 2
- 10 process 212 also provides error detection, correction, and sequenced delivery of all SS7 message packets. I/O queue 214 provides temporary buffering of incoming and outgoing signaling message packets.

GWS process 216 is responsible for examining an incoming signaling message and determining whether triggerless screening service is required.

- 15 In one embodiment, GWS process 216 examines the message transfer part (MTP) origination point code (OPC), destination point code (DPC), and service indicator octet (SIO) parameter values in a received call setup signaling message (e.g., ISUP IAM message) to determine the need for subsequent triggerless screening service processing.
- 20 In the event that a signaling message is identified as requiring ISM service, GWS process 216 encapsulates the incoming signaling message packet within an SS7 signaling connection control part (SCCP) envelope. Figure 3 is a block diagram illustrating an exemplary SCCP-encapsulated MSU that may be generated by GWS process 216 in response to
- 25 determining that the message requires triggerless screening service processing. In Figure 3, an SCCP encapsulating MSU 300 envelops or contains an ISUP MSU 302. Once the ISUP message is encapsulated, the message no longer appears as or is treated as an ISUP message within triggerless screening service routing node 200. Instead, the message is
- 30 processed internally as an SCCP message.. During the encapsulation process, SCCP MSU destination point code (DPC) field 304 is set to the SS7 point code (PC) of the triggerless screening service routing node 200, SCCP

-8-

MSU Called Party Routing Indicator (CdPA RI) field 306 is set to RT-ON-SSN, and SCCP MSU Called Party Subsystem Number (CdPA SSN) field 308 is set to the ISUP service SSN identifier defined within triggerless screening service routing node 200.

- 5 Referring back to Figure 2, once a received call setup message is identified as requiring screening processing and encapsulated within an SCCP packet, the message is passed to HMDC process 218. HMDC process 218 receives the SCCP-encapsulated signaling message from the lower processing layers and performs a discrimination function to determine
- 10 whether the message is addressed to triggerless screening service routing node 200 for internal processing or the message should simply be through switched. Because GWS process 216 identified the message as requiring further call screening processing, GWS process 216 inserts the point code of triggerless screening service routing node 200 in the DPC field of the
- 15 encapsulating SCCP MSU. As a result, HMDC process 218 determines that the message requires further internal processing.

Once HMDC process 218 determines that a message requires internal processing, HMDC process 218 passes the message to HMDT process 220. HMDT process 220 handles the internal routing of SS7 message packets that require additional processing prior to final routing. In this example, HMDT process 220 routes messages requiring triggerless screening service to ISM 210 prior to final routing.

ISM 210 includes databases and control processes necessary to perform the required network address translations to achieve the triggerless ISUP routing functionality implemented by embodiments of the present invention. ISM 210 shown in Figure 2 includes a signaling connection control part (SCCP) process 222, which receives SCCP-encapsulated message packets from IMT bus 202 and de-capsulates and extracts the original SS7 MSUs prior to triggerless screening service processing. SCCP process 222 further includes a triggerless ISUP screening subsystem controller known as a signaling connection routing controller (SCRC) 224. Responsibilities of the SCRC 224 include directing incoming SS7 message

-9-

packets to an IN service selector (SS) database 226, using information returned from SS database 226 to perform a lookup in a service routing (SR) database 228, and modifying the message packets to include routing information returned by SR database 228.

- 5        SCRC process 224 also examines the called party number for the presence of a carrier selection code (CSC) in an E.164-formatted dialed number parameter included within a received SS7 call setup message, such as an ISDN user part (ISUP) initial address message (IAM). If a CSC is present, SCRC process 224 examines a carrier identification code (CID)  
10      contained within the message. A received message may be routed to its original destination without modification if SCRC process 224 determines that the CID belongs to another network, i.e., a network owned by a service provider other than the service provider that owns triggerless screening service routing node 200. Thus, the execution of a service selection lookup  
15      in triggerless screening service routing node 200 and subsequent message redirection may be conditional on the particular carrier specified in a received call setup message.

- SCRC 224 may also examine various parameters in a received call setup message to determine whether triggerless screening service redirection is indicated. These parameters may include the message type indicator in service indicator octet (e.g., ISUP IAM, ISUP REL, etc.), called party address (CdPA) or dialed number (DN), calling party address (CgPA), originating point code (OPC), and destination point code (DPC). The processing of these parameters to determine whether to perform a  
25      triggerless screening service message redirection will be discussed in more detail below.

- SS7 message packets leaving SCRC 224 are received and further processed by a message handling and routing (HMRT) process 230. HMRT process 230 is responsible for the internal routing of SS7 message packets  
30      that do not require additional processing by triggerless screening service routing node 200. That is, HMRT process 230 determines to which LIM or DCM card an SS7 message packet should be routed for subsequent

-10-

outbound transmission. ISM 210 may also be coupled to and serviced by external provisioning and administration platform (EPAP) 231 via an external Ethernet connection. EPAP 231 is responsible for administration and maintenance of the SS and SR databases 226 and 228, respectively.

- 5        Once received call signaling messages are routed by HMRT process 230, the messages travel over IMT bus 202 to the module associated with the external signaling link to which the message is routed. In this example, it is assumed that HMRT process 230 MTP-routes the message to DCM 208. DCM 208 includes an I/O queue 232 for temporarily storing messages to be
- 10      transmitted to or received from an external IP network. An SS7/IP converter process 234 converts outbound messages to IP format and inbound messages to SS7 format. Preferred packet formats for encapsulating SS7 messages in IP packets include the transport adapter layer interface (TALI) for which the source code is available from Tekelec and the stream control
- 15      transmission protocol (SCTP), as described in IETF Request for Comments 2960: Stream Control Transmission Protocol, October 2000. Once DCM 208 routes the message over the external network, the call setup messages that were identified as requiring additional screening service are received and processed by a message processing platform, which will be described in
- 20      detail below.

In Figure 2, SS and SR databases 226 and 228 are co-resident on ISM card 210. These databases may be stored in one or more blocks of high speed random access memory (RAM) located on ISM card 210. Tables 1 and 2 shown below respectively illustrate exemplary contents of databases

- 25      226 and 228.

Table 1: IN Service Selection Database Fields

<u>KEY(s)</u>						<u>DATA</u>
<u>Type</u>	<u>CgPA:DN</u>	<u>CdPA:DN</u>	<u>DPC</u>	<u>OPC</u>	<u>CID</u>	<u>IN Service</u>
IAM	9194605500	*	*	*	*	Credit Limit
IAM	9194691300	*	*	*	*	CallingParty
IAM	*	9194690000	*	*	321	CalledParty
IAM	*	*	1-1-1			

-11-

Table 2: IN Service Routing Database Fields

<u>KEY</u>	<u>ROUTING ADDRESS DATA</u>			
<u>IN Service</u>	<u>PC</u>	<u>SSN</u>	<u>IP Addr</u>	<u>Port</u>
CreditLimit	--	--	101.000.000.001	23
CalledParty_Block	--	12	--	--
CallingParty_Block	5-5-5	12	--	--
OPC_Block	--	--	101000.000.001	21

As indicated by the simplified example presented in Tables 1 and 2, SS  
5 database 226 and SR database 228 may each include a single table. It will  
be appreciated that such a simplistic database structure is presented herein  
purely for the purposes of illustration. In practice, more efficient database  
structures would likely be employed which make use of multiple tables and  
complex binary tree (B-tree) indexing techniques, and, in fact, this  
10 consideration applies to all database and table structures presented herein.

As illustrated in Table 1, service selector database 226 includes a  
number of index or key fields by which the database may be searched. In  
the illustrated example, these key fields include: message type, calling party  
number, called party number, originating point code, destination point code,  
15 and carrier identification code. It will be appreciated that these fields may be  
used alone or in combination as a search or lookup key. With particular  
regard to the calling and called party number fields, it should also be  
appreciated that these parameters may be comprised of conventional  
telephone numbers or Internet-service-related-identifiers. Such Internet  
20 service identifiers may include email addresses, uniform resource locators  
(URLs), or Internet protocol (IP) addresses.

In Table 1, an intelligent network service selector is associated with  
each set of keys. The IN service selector indicates a particular IN service  
that has been provisioned for that key. For example, in the illustrated table,  
25 "CreditLimit" is the IN service selector provisioned for the keys "IAM" and

-12-

"9194605500." A single IN service or more than one IN service may be provisioned for the same key.

As illustrated in Table 2, IN service database 228 is indexed or keyed by the same IN service selector values that are provisioned in the above-  
5 described service selector database. As such, a sample IN service routing record structure includes a service selector key field, a point code field, a subsystem field, an Internet protocol address field, and a port field. It will be appreciated that the point code/subsystem and IP address/port information stored in this table represents a network address corresponding to an IN  
10 message processing platform that is adapted to provide the provisioned call screening service in response to receiving the call setup message. Thus, if a lookup in Table 1 results in "CreditLimit" as the screening service, this value is used in Table 2 to determine the network address of the node that provides credit limit screening service. In Table 2, the network address for  
15 this node is 101.000.000.001, port 23.

#### Exemplary Message Processing Platform Architecture

Figure 4 is a functional block diagram of an intelligent network message processing platform according to an embodiment of the present invention. In Figure 4, message processing platform 400 includes IP/SS7 protocol stacks 400 for sending and receiving both SS7 and IP messages.  
20 An I/O queue 402 buffers messages before inbound or outbound processing can be performed. MPP 400 further includes a service selection manager 406 and a screening manager 408. In this simplified example, screening manager 408 includes a plurality of screening modules 410-422 for screening call setup messages. In Figure 4, screening manager 408 includes a CreditLimit screening module 410, a MissingCallerID screening module 412, an OPC screening module 414, a CallingParty screening module 416, a RedirectingParty screening module 418, a ChargedParty screening module 420, and a CalledParty screening module 422. Screening  
25 modules 410-422 may screen and modify call setup messages, generate SMS messages and billing records, generate new call setup messages, and  
30

-13-

respond on behalf of an end office. Each of these functions will be discussed in detail in the examples discussed below.

Table 3 shown below illustrates an exemplary credit limit screening table used by CreditLimit screening module 414.

5

Table 3: Credit Limit Screening Data

<u>KEY</u>		<u>INSTRUCTION DATA</u>	
<u>Number</u>	<u>Carrier</u>	<u>Billing</u>	<u>SMS</u>
9194691300	*	Yes	Yes
9193457012	636	No	No
9193457894	221	Yes	No
919467****	811	Yes	Yes
212*****	221	No	Yes
770*****	*	No	No

In Table 3, the credit limit screening parameters include a calling party telephone number key field as well as a carrier key field. A billing status field indicates whether a billing record should be created for a received message 10 that matches one of the individual keys or key combinations. Table 3 also includes a short message service indicator field. CreditLimit screening module 410 uses the SMS indicator field to determine whether an SMS message should be generated in response receiving a call setup message, e.g., to notify a calling or called party of the results of a call screening action. 15 SMS message generation may be performed in addition to any modifications made to the original received call setup message.

CreditLimit screening module 410 may utilize the data stored in the credit limit screening table to block or redirect a call attempt and generate an SMS message in response to determining that a calling party has exceed 20 their credit limit with a network operator. For example, in response to receiving a call setup message, CreditLimit screening module 410 may perform a lookup in the credit limit screening table to determine whether the calling party has exceeded his or her credit limit with a particular carrier. In response to determining that a calling party has exceeded his or her credit

-14-

- limit, CreditLimit screening module 410 may block or redirect the call. CreditLimit screening module 410 may also send an SMS message to the calling party or to a short message service center servicing the calling party. The SMS message may indicate that the call was blocked due to a credit problem of the calling party.
- 5

Table 4 shown below illustrates exemplary parameters utilized by MissingCallerID screening module 412.

Table 4: Missing Caller ID Screening Data

<u>KEY</u>		<u>BILLING DATA</u>
<u>CdPA Number</u>	<u>Carrier</u>	<u>Billing</u>
9194691300	221	Yes
9193457312	533	No
9194457894	223	Yes
919469****	841	Yes
212*****	221	No
770*****	*	No

- 10 In the illustrated example, Table 4 includes a called party telephone number key field as well as a carrier key field. A billing status field indicates whether a billing record should be created for a received message that matches one of the individual keys or the key combination.

MissingCallerID module 412 may utilize call screening data, such as that illustrated in Table 4, to block or redirect a call attempt in the event that calling party identification information is missing from a received call setup message. For example, if a particular subscriber does not wish to receive calls from parties that block their caller ID, the subscriber's telephone number may be stored in a table accessible by MissingCallerID module 412.

15

20 When MissingCallerID module 412 receives a message, MissingCallerID module 412 checks the table to determine whether the called party does not wish to receive caller-ID-blocked calls. In response to determining that the called party does not wish to receive calls that lack caller ID information, MissingCallerID module 412 may block or redirect the call setup message.

-15-

- associated with the particular call. It will be appreciated that such a call blocking or redirection service can be activated for blocks or ranges of received call setup messages that are missing calling party identification information through the use of wildcard designators (e.g., "/\*"), such as those
- 5 illustrated in Table 4. In all of the tables described herein, "/\*" denotes a wildcard.

Table 5 shown below illustrates exemplary OPC screening parameters used by OPC screening module 514.

Table 5: OPC Screening Data

<u>KEY</u>		<u>BILLING DATA</u>
<u>OPC</u>	<u>Carrier</u>	<u>Billing</u>
1-1-1	221	Yes
1-1-2	636	No
1-1-3	221	Yes
1-2-*	811	Yes
2-1-1	221	No
3-*-*	*	No

10

- In this example, the OPC screening parameters include an OPC key field and a carrier identification code key field. As with the previous examples, each table entry also includes a billing status indicator that indicates whether or not to generate a billing message in response to a screened call signaling
- 15 message.

15

OPC screening module 414 uses the data illustrated in Table 5 to block or redirect a call attempt in the event that a call setup message originates from a particular switch owned by a particular carrier. For example, OPC screening module 414 may perform a lookup in Table 5 using

20 the OPC extracted from a received ISUP message. If the lookup indicates that the call should be blocked, then OPC screening module 414 either blocks or redirects the call.

Table 6 shown below illustrates exemplary calling party screening parameters used by CallingParty screening module 416.

-16-

Table 6: Calling Party Screening Data

<u>KEY</u>		<u>BILLING DATA</u>	
<u>CpPA Number</u>	<u>Carrier</u>	<u>Billing</u>	<u>SMS</u>
9194691300	221	Yes	Yes
9193657712	636	No	Yes
9193217894	221	Yes	No
9194828888	811	Yes	No
212*****	221	No	Yes
770*****	*	No	No

The calling party screening parameters illustrated in Table 6 include a calling party telephone number key field and a carrier identification code key field.

- 5    Each entry in Table 6 also includes an SMS indicator and a billing status indicator to indicate whether to send an SMS message and whether to generate billing information for a received call setup message.

CallingParty screening module 416 uses the data stored in Table 6 to block or redirect a call attempt in the event that a call setup message is  
10    received that is associated with particular calling party. For example, calling party screening module 416 may perform a lookup in Table 6 based on the calling party address in a received signaling message. If the address matches one of the entries in the table, then CallingParty screening module 416 may block or redirect the call and send an SMS message to the calling party.  
15    The asterisks in Table 6 indicate that call screening can be performed based on ranges of calling party numbers.

Table 7 shown below illustrates exemplary redirecting number screening data that may be used by RedirectingNumber screening module 418.

20              Table 7: Redirecting Number Screening Data

<u>KEY</u>		<u>BILLING DATA</u>
<u>Redirecting Number</u>	<u>Carrier</u>	<u>Billing</u>
9194691300	221	Yes

-17-

9193657712	636	No
9193217894	221	Yes
9194828888	811	Yes
212*****	221	No
770*****	*	No

In the illustrated example, Table 7 includes a redirecting number key field and a carrier identification code key field. Each entry also includes a billing data field that indicates whether to generate a billing record.

- 5        In operation, RedirectingNumber screening module 418 uses the data in Table 7 block or redirect a call attempt in the event that a call setup message is received from a particular redirecting number. For example, when redirecting number screening module 418 receives a call setup message, RedirectingNumber screening module 418 may extract the
- 10      redirecting number from the message and perform a lookup in a table similar to Table 7 based on the redirecting number. If the redirecting number from the message matches one of the entries, RedirectingNumber screening module 418 may block or screen the call based on the content of the entry.
- 15      RedirectingNumber screening module 418 may also generate a billing record if the billing indicator for that particular entry indicates that such a record should be generated.

Table 8 shown below contains exemplary data used by ChargedParty screening module 420.

Table 8: Charged Party Screening Data

<u>KEY</u>		<u>BILLING DATA</u>
<u>Number</u>	<u>Carrier</u>	<u>Billing</u>
9194691300	221	Yes
9193657712	636	No
9193217894	221	Yes
9194828888	811	Yes
212*****	221	No
770*****	*	No

-18-

- In this example, a charged party screening table includes a telephone number key field for storing charged party numbers and a carrier identification code key field for storing carrier identifiers. As with the 5 previous examples, each entry in the table may include a billing indicator for indicating whether a billing record should be generated for the call.

ChargedParty screening module 420 uses the data in Table 8 to block or redirect a call attempt in the event that the party that is paying for the call is in the list of prohibited callers. For example, when ChargedParty 10 screening module 420 receives a call setup message, ChargedParty screening module 420 extracts the telephone number corresponding to the charged party from the call setup message and performs a lookup in Table 8 based on the extracted number. In response to locating a matching entry in Table 8, ChargedParty screening module 420 may block or redirect the call.

15 Table 9 shown below illustrates exemplary CalledParty screening data used by CalledParty screening module 422.

Table 9: Called Party Screening Data

<u>KEY</u>		<u>BILLING DATA</u>	
<u>CgPA Number</u>	<u>Carrier</u>	<u>Billing</u>	<u>SMS</u>
9194691300	221	Yes	Yes
9193657712	636	No	Yes
9193217894	221	Yes	No
9194828888	811	Yes	No
212*****	221	No	Yes
770*****	*	No	No

In this example, the called party screening table includes a called party 20 telephone number key field for screening called party numbers in received call signaling messages and a carrier identification code key field for storing a carrier identifier. Each entry may also include a billing indicator for indicating whether a billing record is required to be generated for the call.

-19-

- In operation, CalledParty screening module 422 utilizes data in Table 9 to block or redirect a call attempt to a prohibited called party. For example, when CalledParty screening module 422 receives a call setup message, CalledParty screening module 422 extracts the called party ID from the 5 message and performs a lookup in Table 9 based on the called party ID. In response to locating a matching entry, CalledParty screening module 422 may block or redirect the call and possibly generate a billing record, depending on the content of the billing record field.

The present invention is not limited to the IN screening service 10 described above. Numerous other types of IN or IN-like services may be provided by MPP 500 in the same manner as the IN screening services described above. Each of the screening modules may also generate a second, new message in response to screening a call setup message. Such 15 a new message may be another SS7 call setup message, a call setup message of a different protocol (e.g., session initiation protocol), or a non-call setup message (e.g., short message service, transaction capabilities application part message, mobile application part message, etc.).

Returning to Figure 4, modules 408-422 communicate with a diversion prefix (DP) database 426 and a usage measurements and billing (UMB) database 428 to obtain diversion prefixes and billing information for received call setup messages. Diversion prefix database 426 stores 20 information used to modify and divert a call setup message in response to determining that the message satisfies (or fails, depending upon the particular implementation) one or more of the provisioned IN screening services. The information obtained from diversion prefix database 426 may 25 also indicate to the receiving node the results and type of call screening action performed. Usage measurements and billing database 428 stores exemplary data that may be used to generate billing records. Exemplary data that may be stored in databases 426 and 428 will now be discussed in 30 more detail.

Table 10 shown below illustrates an exemplary diversion prefix parameters.

-20-

Table 10: Diversion Prefix Data

<u>KEY</u>				<u>DIVERSION PREFIX</u>
<u>Service</u>	<u>Number</u>	<u>OPC</u>	<u>Carrier</u>	<u>Prefix</u>
CreditLimit	*	*	*	867
MissingCallerID	*	*	*	745
CallingParty	*	*	*	201
OPC	*	*	*	978
CalledParty	*	*	*	351
RedirectingParty	*	*	*	204
ChargedParty	*	*	*	512

As illustrated above, each entry in the diversion prefix table includes a service type key field and an associated diversion prefix that is used to

- 5 modify a screened call setup and cause the message to be redirected or diverted from its originally intended route. Such call setup message diversion may be used to block or redirect a call attempt, and/or to invoke an interactive voice response (IVR) node. IVR nodes are typically deployed in communication networks to play pre-recorded messages to a calling party.
- 10 In the case of a call block initiated by MPP 200, an IVR node may be engaged to play a pre-recorded message that informs the calling party of the reason that the call was blocked, e.g., due to the called party's credit standing with the telecommunications service provider.

Usage measurements and billing database 428 includes a table of usage metrics and billing information related to the screening and processing of call setup messages by MPP 200. In one embodiment, usage measurements and billing database 426 maintains call detail records (CDRs) of screened messages. Table 11 shown below illustrates an exemplary usage measurements and billing data for screened messages.

-21-

Table 11: Usage Measurements and Billing Data

<u>KEY</u>			<u>BILLING RECORD DATA</u>	
<u>Date</u>	<u>Time</u>	<u>Service</u>	<u>Number</u>	<u>Carrier</u>
12/01/2000	13:01:24	CallingParty	9194591300	221
12/01/2000	13:01:26	CalledParty	9193457012	616
12/01/2000	13:01:34	OPC	9193457894	221

As illustrated above, each entry in the usage measurements and billing table includes date, time, and service type key fields. Each entry may also include

- 5 a phone number field that contains the phone number or identifier (e.g., email address, URL, etc.) used in the screening process. Each entry may further include a carrier ID field for storing the carrier ID associated with the screened message. Although not illustrated in Table 10, usage measurements and billing database 428 may also store peg count
- 10 information.

Exemplary Internal Message Processing by Triggerless Screening Service

Routing Node

- Figures 5A and 5B are a flow chart illustrating message processing performed by triggerless screening service routing node 200 illustrated in
- 15 Figure 3. Referring to Figure 5A, in step **ST1**, an incoming ISUP IAM message is received at inbound LIM module 206. In steps **ST2** and **ST3**, the incoming ISUP IAM message is received and processed by the MTP Level 1 and 2 process 212. As stated above, MTP level 1 and 2 processing includes error detection, error correction, message sequencing, etc. When MTP
- 20 Level 1 and 2 processing is completed, the IAM message is temporarily buffered in I/O queue 214 before being passed up the stack to gateway screening process 216. In step **ST4**, GWS process 216 examines the ISUP IAM message and determines not only whether the message is to be allowed into the switch for further processing, but also whether further
- 25 triggerless screening service processing of the message is required. In this example, GWS process 216 examines the incoming ISUP IAM message and determines that the message is permitted to enter the switch. In step **ST5**,

-22-

GWS process 216 examines the originating point code (OPC) and service indicator (SI) fields contained in the MTP routing layer of the message and determines that the message requires additional triggerless screening service processing by ISM 210.

- 5        After verifying that the received message is an ISUP message signaling unit (MSU), in step ST6, GWS process 216 encapsulates the ISUP MSU within an SCCP envelope. Such SCCP encapsulation may be achieved by adding SCCP message leading and trailing bit sequences to the base bit sequence of the ISUP IAM MSU, as illustrated in Figure 3. Thus, an  
10      SCCP encapsulating MSU is created which envelops or contains an ISUP MSU.

- After the ISUP message is encapsulated in the SCCP envelope, the message is no longer treated as an ISUP IAM message within triggerless screening service routing node 200, but is instead processed internally as an
- 15      SCCP message. As mentioned previously, during the encapsulation process, the SCCP MSU destination point code (DPC) field is set to the point code of triggerless screening service routing node 200, the SCCP MSU called party routing indicator (CdPA RI) field is set to subsystem number (SSN), and the SCCP MSU called party subsystem number (CdPA SSN)  
20      field is set to the subsystem number corresponding to ISM 210. It should also be appreciated that failure of the incoming ISUP MSU to meet the criteria specified in step ST5 causes the original, non-encapsulated MSU to be routed directly to HMDC process 316 where normal MSU routing is resumed.
  - 25      However, in the case where an incoming MSU satisfies the step ST5 criteria (i.e., ISUP MSU from a designated OPC), SCCP encapsulation of the MSU occurs and the resulting encapsulated MSU is directed to HMDC process 218, where the message is identified as requiring further internal processing (ST7). HMDC process 218 examines the message packet and  
30      determines that the DPC of the packet is the PC of triggerless screening service routing node 200. Consequently, further processing of the SCCP MSU within triggerless screening service routing node 200 is assumed to be

-23-

- necessary, and the packet is passed to the HMDT process 220. HMDT process 220 examines the service indicator (SI) field of the message, which indicates that encapsulating packet is of an SCCP type. As such, HMDT process 218 places encapsulating SCCP MSU 370 on high speed IMT bus 202 for transport to ISM 210 and subsequent triggerless screening service processing.

Referring now to Figure 5B, in step **ST8**, the encapsulating SCCP MSU is received and verified by SCCP process 224. The SCCP message is next passed to SCRC process 226, where it is verified that the SCCP MSU contains an encapsulated ISUP MSU. Such verification processing may include the verification of the pointers and field lengths associated with the ISUP message. In the event that the contents of the encapsulating packet are determined to be something other than an ISUP signaling message, the packet is passed to HMRT process 230 for outbound routing or possibly further processing at another card on the IMT bus 202. Following a positive ISUP verification, the original ISUP MSU is extracted by removing and discarding the SCCP wrapper (**ST9**).

Once the ISUP MSU is extracted, in step **ST10**, a lookup is performed in service selector database 226 using information extracted and/or inferred from the original ISUP MSU. Database 226 may be searched by comparing parameters extracted from the ISUP message to at least one of the keys contained in SS database 226 (e.g., message type, calling party number, called party number, OPC, DPC, CID, etc.). In step **ST11**, ISM 210 determines whether a matching entry has been located. If a matching entry is found, in step **ST12**, a lookup is performed in service routing database 228. Database 228 may be searched by comparing parameters extracted from the message to the IN service information stored in database 228.

The resulting matching entry in IN service routing database 228 yields routing instructions that are to be applied to the received ISUP MSU. These routing instructions may include an SS7 point code and subsystem or an Internet protocol (IP) address and port. Once the routing address is located, the routing label of the original ISUP MSU is modified to reflect the new

-24-

- routing instructions (**ST13**), and the message is passed to HMRT process 350 (**ST14**) for subsequent routing to the outbound DCM 208 (**ST15**). In this particular example, DCM 208 encapsulates the modified ISUP MSU in a transport adapter layer interface packet for transmission via a TCP/IP connection or socket to an associated IN message processing platform (MPP), as indicated in step **ST16**. Information identifying the required IN service or services may be included in the TALI component of the encapsulated ISUP packet. Accordingly, a triggerless screening service routing node of the present invention is adapted to intercept and redirect a call setup message to a MPP for subsequent IN-type processing.

Exemplary Internal Message Processing by MPP 400

- Figure 6 is a flow chart illustrating exemplary steps performed by MPP 400 in providing triggerless IN screening service according to an embodiment of the present invention. Referring to Figure 6, in step **ST1**, MPP 400 extracts the carrier number from the called party digits in a received ISUP message. The purpose of extracting the carrier number is to determine whether the owner of MPP 400 has a service agreement to provide triggerless IN services for the particular carrier identified by the carrier ID. Accordingly, in step **ST2**, MPP 400 determines whether the carrier number is unknown. If the carrier number is unknown, in step **ST3**, MPP 400 returns the original IAM message to triggerless screening service routing node 200, which forwards the message to the called party end office.

- In step **ST4**, if the carrier number is not unknown, i.e., if the particular carrier has a service agreement with the owner of MPP 400, MPP 400 extracts the originating point code from the IAM message. The originating point code indicates a particular switching system within the carrier's network from which the IAM message originated. In step **ST5**, MPP 400 extracts screening options for the particular carrier. Such screening options may include credit limit screening, missing caller ID screening, OPC screening, calling party screening, redirecting party screening, charged party screening, or called party screening. In this example, it is assumed that OPC and calling party screening are provisioned for this particular carrier.

-25-

Accordingly, in step **ST6**, MPP 400 determines whether the carrier is screening this particular OPC.

According to an important aspect of the invention, in step **ST7**, if the carrier is screening this particular OPC, MPP 400 obtains an OPC screening identifier for the particular carrier. The identifier indicates which screening criteria are matched by MPP 400. In step **ST8**, MPP 400 inserts the identifier into the IAM message. The screening identifier may be inserted as a prefix in the called party number field of the IAM message. The identifier will be used by the receiving end office to identify the type of screening action performed by MPP 400 and the result of the screening action. The receiving end office may use the identifier to take appropriate action, such as contacting an IVR node. In step **ST9**, MPP 400 returns the modified IAM message to triggerless screening service routing node 200. Triggerless screening service routing node 200 forwards the modified message to the destination end office.

Inserting an identifier in an IAM message at a message processing platform that is separate from an originating end office eliminates the need for end office triggered IN services. Traditionally, such services have required that each end office determine whether a dialed number requires IN service, formulate a TCAP query to a service control point to determine the type of service required, receive a TCAP response from the service control point, and then provide the appropriate IN service. The trigger for the IN service must be provisioned for each number requiring IN service at each end office. Thus, associating such services with subscriber numbers requires that each end office be provisioned to recognize numbers requiring IN services. Provisioning all such end offices is labor intensive and often impossible when the end offices are owned by different carriers. Triggerless screening service routing node 200 and MPP 400 according to embodiments of the present invention eliminate this problem by centralizing the numbers that require IN services and inserting a prefix that a particular carrier can use to recognize an IN service required for a call.

-26-

In addition to OPC screening services, MPP 400 may perform other screening operations, such as calling party screening. Accordingly, in step ST10 in Figure 6, MPP 400 extracts the calling party number from the IAM message. In step ST11, MPP 400 determines whether the calling party  
5 number is missing from the IAM message, such as when the calling party blocks such information. In step ST12, MPP 400 extracts a missing automatic number identification error identifier for the particular carrier. In step ST13, MPP 400 inserts the identifier into the IAM message. In a preferred embodiment of the invention, the message is inserted as a prefix in  
10 the called party number field of the IAM message. In step ST14, the IAM message is returned to triggerless screening service routing node 200, which forwards the message to its intended destination.

As indicated in Figure 6, additional screening checks may be performed. Accordingly, by inserting an identifier or identifiers into a  
15 received IAM message that indicate the type of screening and the outcome of the screening performed by MPP 400, MPP 400 according to an embodiment of the present invention reduces both provisioning and processing requirements at end office switching systems.

Message Processing Platform Internal Message Flow

20 Referring back to Figure 4, the dotted line illustrates an exemplary message flow path through message processing platform 400 according to an embodiment of the present invention. In the example in Figure 4, it is assumed that MPP 400 receives an IP-encapsulated ISUP packet via a TCP/IP socket connection. SS7/IP protocol stacks 402 receive the packet  
25 and extract the ISUP MSU payload contained therein. The extracted ISUP MSU is then passed via I/O queue 404 to service selection manager 406. Service selection manager 406 examines destination address information (e.g., DPC and SSN) contained within the ISUP message to determine the particular IN service or services that are required.

30 It will be further appreciated that such destination address information may be used not only to identify a particular IN service, but also to specify a particular screening variation. For example, a particular point code and

-27-

subsystem in a received ISUP message may indicate that the received message requires credit limit screening. Once, service selection manager identifies the type of screening service(s) required, service selection manager 406 passes the message to CreditLimit screening module 410 of screening module 408. CreditLimit screening module 410 examines the ISUP message and extracts calling party number information from the message. For the purposes of this example, it is assumed that the calling party number is 919-469-1300. CreditLimit screening module 408 uses the extracted calling party number to perform a lookup in the credit limit screening table (Table 3). As illustrated in Table 3, a search of the number field for 919-469-1300 results in the location of a match with the first entry in the credit limit screening table. This matching entry in the table also indicates that a usage measurements/billing record should be generated. Consequently, a copy of the ISUP MSU or a portion of the information contained therein is passed to usage measurements and billing (UMB) database 428, where an entry is inserted in a UMB table, as indicated in Table 11. Such UMB data may be used at a later time to generate invoices for the use of MPP resources.

CreditLimit screening module 410 also communicates with diversion prefix database 426 to obtain a prefix to be used for diversion or redirection of the ISUP MSU. CreditLimit screening module 410 appends the diversion prefix to the called party number contained in the original ISUP MSU. It will be appreciated that in the particular example discussed herein, only the IN service type is required to obtain diversion or redirection instructions for the ISUP MSU, as all other specifying parameters are wildcards in diversion prefix database 426.

The terms "diversion prefix" and "screening identifier" are used interchangeably herein. Both phrases are intended to refer to a parameter that is inserted in the call setup message that identifies the type and result of a screening action to a destination node. The destination node may use this parameter or parameters to take appropriate action, such as blocking or redirecting a call.

-28-

- Referring to Table 10 set forth above, a lookup based on the number 919-469-1300 results in a diversion prefix value of 867, which indicates that credit limit screening was performed and that the message failed the credit limit screening process. CreditLimit screening module 410 obtains the
- 5 diversion prefix value from diversion prefix database 426 and appends this information to the called party number contained in the original ISUP MSU. CreditLimit screening module 410 may also add or modify several additional parameters contained within the ISUP MSU, including: an original called number (OCN) parameter, a redirecting number (RN) parameter, a
- 10 redirection information (RI) parameter, and a forward call indicator (FCI) parameter. The OCN parameter is used to maintain a copy of the original called number within the ISUP MSU. The RN parameter is used to track the "exchange" that performed the MSU diversion. The RI parameter is used to count the total number of times the call has been redirected along with the
- 15 reason for each redirection, and the FCI is modified to a value that indicates "ISUP preferred all the way" so that the call diversion/redirection information is not lost. It should be appreciated that other parameters may be modified or added to an ISUP MSU, depending upon the particular IN service processing that is involved.
- 20 In any event, the modified ISUP MSU is then passed to SS7/IP protocol stack 402 for encapsulation within a TALI packet. The IP-encapsulated, modified ISUP MSU is then transmitted back to triggerless screening service routing node 200 for subsequent routing to a final destination. Again, it will be appreciated that TALI encapsulation is not an
- 25 essential element or requirement of the present invention but instead simply facilitates the transmission of ISUP MSUs via a TCP/IP socket connection as opposed to a conventional SS7/MTP type signaling link.

-29-

Call Screening Examples

Figure 7 illustrates an exemplary communication network including network elements and message flows of a system for providing triggerless IN services according to an embodiment of the present invention. In Figure 7,

5 network 700 includes triggerless screening service routing node 200 and MPP 400 described above. Communications network 700 also includes a number of discrete network elements and communication terminals, including an originating end office 702, a second EO 704, a tandem office 706, a calling party 708, and a called party 710. An interactive voice

10 response node 712 receives digits from and plays pre-recorded messages to a calling party. In the case of a call block initiated by a system for providing triggerless IN services according to embodiments of the present invention, such an IVR node may be engaged to play a pre-recorded message that informs the calling party of their poor credit standing, or similar type

15 information.

In this example, it is assumed that CallingParty blocking service is desired and has consequently been provisioned in MPP 400 by the owner/operator of network 700. When calling party 708 attempts to place a call to called party 710, end office 702 generates an ISUP initial address message (IAM) M1. Message M1 is transmitted to triggerless screening service routing node 200, where GWS process 216 examines the MSU and determines that further internal processing is required by ISM module 210. ISM module 210 processes the MSU and determines that further processing is required by MPP node 400. Again, such a determination is made through

20 a search of the service selector and service routing databases based on the calling party number (i.e., 919 469-1300).

25

Once the message is identified as requiring further processing by MPP 400, the message M1 is TALI-encapsulated and forwarded to MPP node 400 for subsequent processing as message M2. MPP node 400 receives TALI-encapsulated message M2 and extracts the ISUP IAM MSU contents. The ISUP IAM MSU is eventually processed by CallingParty screening module 416. As generally indicated in Table 6, the calling party

30

-30-

- has been identified as blocked party. That is, calls from this party are not to be allowed in the network 700. Furthermore, as indicated by the billing identifier for the matching entry in Table 6, a record of this transaction is required. Consequently, a billing record is generated in UMB database 428
- 5 to track this IN service transaction and a diversion prefix "201" is obtained from DP database 428 is included in the ISUP IAM MSU. Other parameters within the original ISUP IAM MSU may also be changed or added to complete the MSU modification process, as discussed previously.

Table 12 shown below includes a partial listing of the parameter  
10 contents of the original (M2) and modified (M3) ISUP IAM MSU.

Table 12: Original and Modified ISUP Message Contents

PARAMETER	M2	M3
CGPA Number	9194691300	9194691300
CDPA Number	9193803815	DP+9193803816

In Table 12, the leftmost column indicates the parameter names for some of the parameters in an ISUP MSU. The central column illustrates the parameters of the message M2. The rightmost column illustrates the 15 parameters of the message M3 after processing by MPP 400. It can be seen by comparing the parameters of messages M2 and M3 that MPP 400 has inserted a screening type identifier, which is symbolically illustrated by "DP" in message M3, that can be used by the receiving end office to determine the type and outcome of the screening performed by MPP 400  
20 and to take appropriate action. In addition to or instead of adding the screening type identifier to the called party number, MPP 400 may modify the called party number. In example illustrated in Table 12, the called party number has been changed from 9193803815 to 9193803816. The new called party number may be used by the receiving end office to direct the call  
25 to an operator or customer service agent who will explain the result of the screening action to the caller. If the original called party number is modified, MPP 400 may also store the original called party number in the call setup message.

-31-

Referring back to Figure 7, once message M3 is modified to include the screening service identifier, the message is TALI-encapsulated and transmitted back to triggerless screening service routing node 200 for routing. In this particular example, the modified ISUP IAM MSU is extracted

5 from message M3 at the triggerless screening service routing node 200, and the modified ISUP IAM MSU is then routed to tandem office 706 as message M4. Tandem office 706 receives message M4 and determines the type and outcome of the screening performed by MPP 400 based on the screening identifier. In this example, it is assumed that calling party screening was

10 performed and that the number was screened. Accordingly, tandem office 706 subsequently generates a new ISUP call setup message M5, which is routed via triggerless screening service routing node 200 to EO 704. EO 704 may then instruct IVR node 712 to play an announcement to the caller indicating results of the screening action. Because the message M4

15 includes the screening type identifier and/or the modified called party number, tandem 706 and end office 704 know the type and results of the screening action and can take appropriate action.

In this example, the attempt by calling party 708 to contact called party 710 is unsuccessful, because the ISUP call setup messages associated with this call attempt are modified by MPP 400. Tandem 706 and/or EO 704 may then direct IVR node 712 to play a message to the caller. The IVR system may notify the calling party that the call has been blocked and the associated reason for the blocking. Because MPP 400 inserts a screening identifier in the IAM message that indicates the type and outcome of the screening performed by MPP 400, there is no need for an originating end office trigger.

The methods and systems described herein for providing triggerless screening services may be applied to screen calls in mobile communications networks. Figure 8 is a network diagram illustrating a mobile communications network and an example of mobile screening service provided by embodiments of the present invention. In Figure 8, a mobile communications network 800 handles calls from a wireless or mobile

-32-

subscriber 802. As such, network 800 includes a base station system (BSS) 804 and a corresponding mobile switching center (MSC) node 806. A BSS essentially provides the air-interface in wireless communication networks. An MSC provides basic switching functionality and coordinates the establishment of calls between wireless end users. An MSC is directly responsible for transmission facilities management, mobility management, and call processing functions. An MSC is typically in communication with the air-interface components of a wireless network (i.e., base station systems) as well as with other voice and signaling related nodes in the wireless network. As such, an MSC includes switching functions, mobile application functions, and other service logic functions in a wireless communications network.

Network 800 also includes a short message service center (SMSC) 810. Short message service center 810 serves as a store and forward center for short message traffic in the network. As such, a call attempt to the called party 710 that is made by mobile calling party 802 results in the generation of an ISUP initial address message (IAM) M1 by the serving or originating MSC 806. This call setup message is received and processed by triggerless screening service routing node 200 in a manner that is similar to that described with regard to Figure 7. Consequently, the message is encapsulated and diverted to MPP node 400 for IN service processing as message M2. In this case, CallingParty service processing at MPP node 400 results in additional step of generating a short message service (SMS) message M3 that is subsequently TALI-encapsulated and transmitted back to triggerless screening service routing node 200. Triggerless screening service routing node 200 receives the encapsulated message and routes the SMS message to the SMSC node 810 as message M4.

SMSC node 810 receives SMS message M4 and delivers the message to calling party 802. Again, it will be appreciated that such an SMS message may include a text message that indicates some information associated with the blocking incident to the calling party 802. Because MPP node 400 automatically generates the SMS message indicating the results of

-33-

- the screening action, the calling party is notified of the screening and make other arrangements for contacting called party 710 or contact the owner of MPP 400 to determine the reason for the screening action. This message is particularly useful if the calling party is screened because of failure to pay a bill. Once the calling party pays the bill, the owner of MPP 400 can remove the block and allow calls from the particular party to proceed. Removing the block simply involves modifying one database in MPP 400 versus modifying databases at each end office, as required by prior art trigger-based screening systems. Thus, the present invention reduces the burden on network operators in providing and maintaining screening services.

The methods and systems for providing triggerless IN screening services described herein reduce the need for end office triggers and reduce network traffic. By redirecting call setup messages to a message processing platform, the methods and systems described herein render TCAP-based screening services obsolete. By inserting a screening identifier in a screened ISUP message, the methods and systems described herein communicate call screening information to destination nodes.

It will be understood that various details of the invention may be changed without departing from the scope of the invention. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation—the invention being defined by the claims.

-34-

CLAIMS

What is claimed is:

1. A system for providing triggerless access to intelligent network services in a communications network, the system comprising:
  - 5 (a) a triggerless screening service routing node for determining whether received messages require call screening processing and for diverting the messages that require call screening processing from their original destinations; and
  - 10 (b) a message processing platform (MPP) operatively associated with the triggerless screening service routing node for receiving the diverted messages, performing at least one call screening action on each of the diverted messages, modifying each message to indicate results of the call screening action and forwarding each modified message to a destination node.
2. The system of claim 1 wherein the triggerless screening service routing node is adapted to determine whether the received messages require call screening processing based on whether the received messages comprise call setup messages and, in response to determining that a received message is a call setup message, for diverting the call setup message to the message processing platform.
- 20 3. The system of claim 1 wherein the triggerless screening service routing node is adapted to determine whether the received messages comprise ISUP messages, and in response to determining that a received message is an ISUP message, for diverting the ISUP message to the message processing platform.
- 25 4. The system of claim 1 wherein the triggerless screening service routing node is adapted to determine whether the received messages comprise ISUP IAM messages, and in response to determining that a received message comprises an ISUP IAM message, for diverting the ISUP IAM message to the message processing platform.
- 30

-35-

5. The system of claim 1 wherein the triggerless screening service routing node is adapted to determine whether the received messages comprise SIP messages, and, in response to determining that a received message is a SIP message, for diverting the SIP message to the message processing platform.
10. The system of claim 1 wherein the triggerless screening service routing node is adapted to determine whether the received messages comprise SIP INVITE messages, and, in response to determining that a received message is an INVITE message, for diverting the INVITE message to the message processing platform.
15. The system of claim 1 wherein the triggerless screening service routing node comprises a signal transfer point.
20. The system of claim 1 wherein the triggerless screening service routing node comprises an SS7/IP gateway.
25. The system of claim 1 wherein the message processing platform includes a service selection manager for determining a type of screening required for each of the diverted messages.
30. The system of claim 1 wherein the message processing platform comprises a screening manager including a plurality of screening modules for performing the call screening actions.
11. The system of claim 10 wherein the screening manager includes a credit limit screening module for screening a call setup message diverted by the triggerless screening service routing node in response to determining that a calling party's credit with a telecommunications service provider exceeds a predetermined limit.
12. The system of claim 10 wherein the screening manager includes a missing caller ID screening module for screening a call setup message diverted by the triggerless screening service routing node that lacks caller identification information in response to determining that a called party does not wish to receive calls that lack caller identification information.

-36-

13. The system of claim 10 wherein the screening manager includes a calling party screening module for screening a call setup message diverted by the triggerless screening service routing node in response to determining that the calling party identified by the call setup message is in a predetermined list of calling parties.  
5
14. The system of claim 10 wherein the screening manager includes a redirecting party screening module for screening a call setup message diverted by the triggerless screening service routing node in response to determining that the redirecting party identified by the call setup message is in a predetermined list of redirecting parties.  
10
15. The system of claim 10 wherein the screening manager includes a charged party screening module for screening call setup messages diverted by the triggerless screening service routing node based on the charged party identified by the call setup messages.
- 15 16. The system of claim 10 wherein the screening manager includes a called party screening module for screening a call setup message diverted by the triggerless screening service routing node based on a called party identified by the call setup message.
17. The system of claim 10 wherein the screening manager is adapted to determine whether to create a billing record for a call setup message diverted by the triggerless screening service routing node.  
20
18. The system of claim 10 wherein the screening manager is adapted to generate and forward a message to a calling party indicating results of the call screening action.
- 25 19. The system of claim 18 wherein the calling party comprises a mobile telecommunications system subscriber and the message comprises a short message service (SMS) message.
20. A method for providing triggerless screening services in a communications network, the method comprising:  
30
  - (a) receiving a call setup message;
  - (b) determining whether the call setup message requires call screening processing;

-37-

- (c) in response to determining that the call setup message requires call screening processing, diverting the call setup message to a message processing platform;  
at the message processing platform:
  - 5 (d) performing at least one screening action on the call setup message;
  - (e) modifying the call setup message to identify the type and result of the screening action; and
  - (f) forwarding the call setup message to a destination node.
- 10 21. The method of claim 20 wherein receiving a call setup message includes receiving an ISUP IAM message.
- 22. The method of claim 20 wherein receiving a call setup message includes receiving a SIP INVITE message.
- 23. The method of claim 20 wherein receiving a call setup message  
15 includes receiving a call setup message from an end office.
- 24. The method of claim 20 wherein receiving a call setup message includes receiving a call setup message from a mobile switching center.
- 25. The method of claim 20 wherein determining whether the message  
20 requires call screening processing includes examining a message type of the call setup message.
- 26. The method of claim 20 wherein diverting the call setup message to the message processing platform includes encapsulating the call setup message in an IP packet and forwarding the IP packet to the  
25 message processing platform.
- 27. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing credit limit screening on the call setup message.
- 28. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing missing caller  
30 ID screening on the call setup message.

-38-

29. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing calling party screening on the call setup message.
30. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing OPC screening on the call setup message.
- 5 31. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing charged party screening on the call setup message.
- 10 32. The method of claim 20 wherein performing at least one screening action on the call setup message includes performing called party screening on the call setup message.
33. The method of claim 20 wherein modifying the call setup includes modifying the message to include a diversion prefix usable by an end office or a tandem office to redirect the call setup message from its intended destination.
- 15 34. The method of claim 20 wherein modifying the call setup message includes inserting the screening identifier in a called party number field of the call setup message.
- 20 35. The method of claim 20 wherein the call setup message includes an original called party number modifying the call setup message includes modifying the original called party number in the call setup message.
36. The method of claim 35 comprising storing the original called party number in the call setup message.
- 25 37. The method of claim 20 wherein forwarding the call setup message to a destination node comprises forwarding the call setup message to an end office.
38. The method of claim 20 wherein forwarding the call setup message to a destination node includes forwarding the call setup message to a tandem office.
- 30

-39-

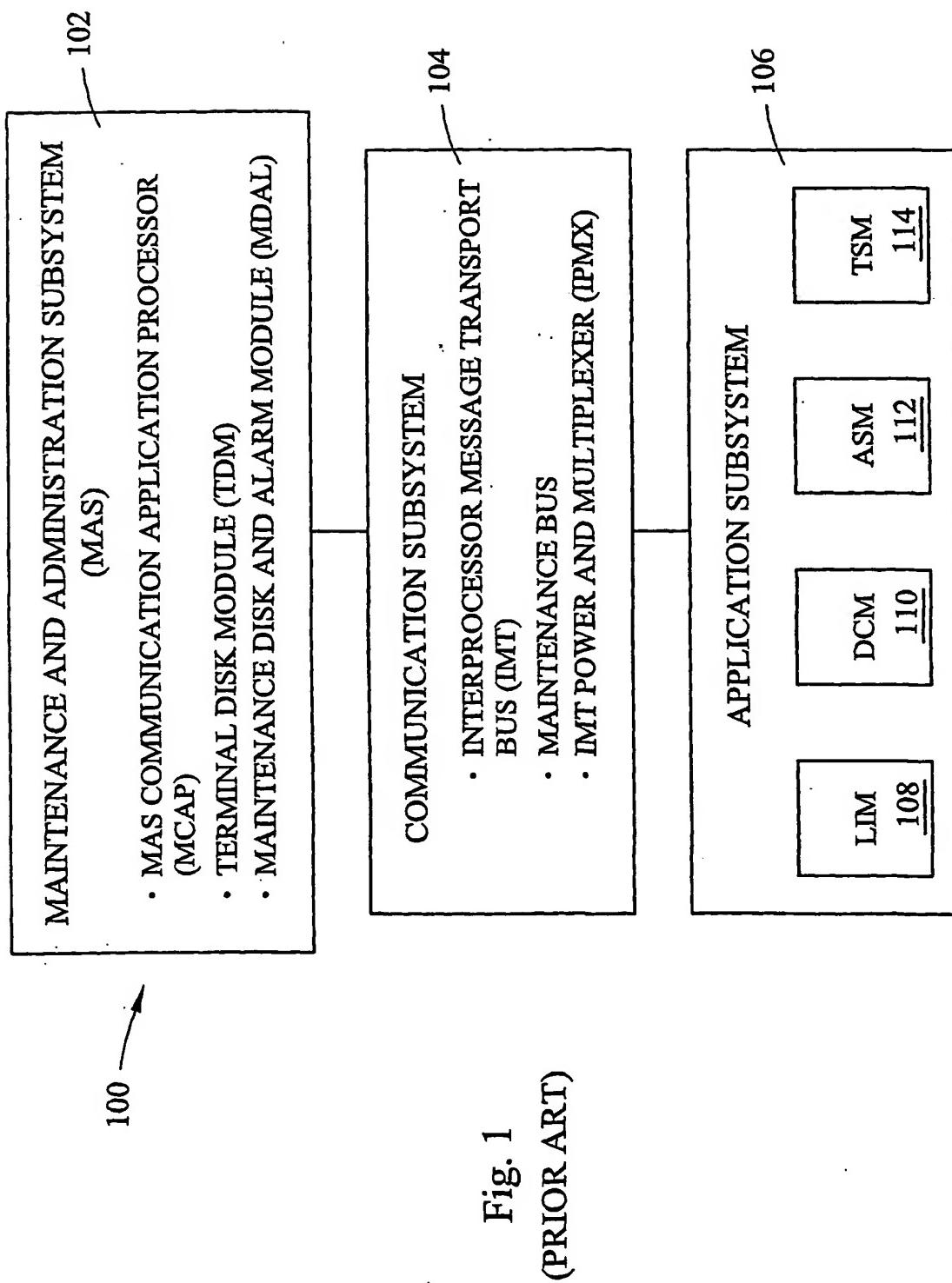
39. The method of claim 20 further comprising generating a billing record based on the call setup message.
40. The method of claim 20 further comprising generating a short message service message indicating results of the screening action.
- 5 41. A method for providing triggerless screening services in a communications network, the method comprising:
  - (a) receiving a call setup message;
  - (b) identifying the call setup message as an ISUP message and, in response, forwarding the ISUP message to a database;
  - 10 (c) performing a lookup in the database based on one or more parameters in the call setup message to identify a screening service required for the call setup message;
  - (d) performing the screening action on the call setup message;
  - (e) modifying the call setup message to include results of the screening action; and
  - 15 (f) forwarding the call setup message to a destination node.
42. The method of claim 41 wherein receiving a call setup message includes receiving a call setup message at a signal transfer point.
43. The method of claim 41 wherein receiving a call setup message includes receiving a call setup message at an SS7/IP gateway.
- 20 44. The method of claim 41 wherein performing a lookup based on one or more parameters in the call setup message includes performing a lookup based on a carrier ID in the call setup message.
45. The method of claim 41 wherein performing a screening action includes performing at least one of: credit limit screening, missing caller ID screening, OPC screening, calling party screening, redirecting party screening, charged party screening, and called party screening.
- 25 46. The method of claim 41 wherein forwarding the call setup message to a destination node includes forwarding the call setup message to an end office and wherein the end office uses the results of the screening
- 30

-40-

action to instruct an interactive voice response (IVR) node to play a message to the calling party.

47. The method of claim 41 comprising generating a short message service message indicating results of the screening action.

1/9



2/9

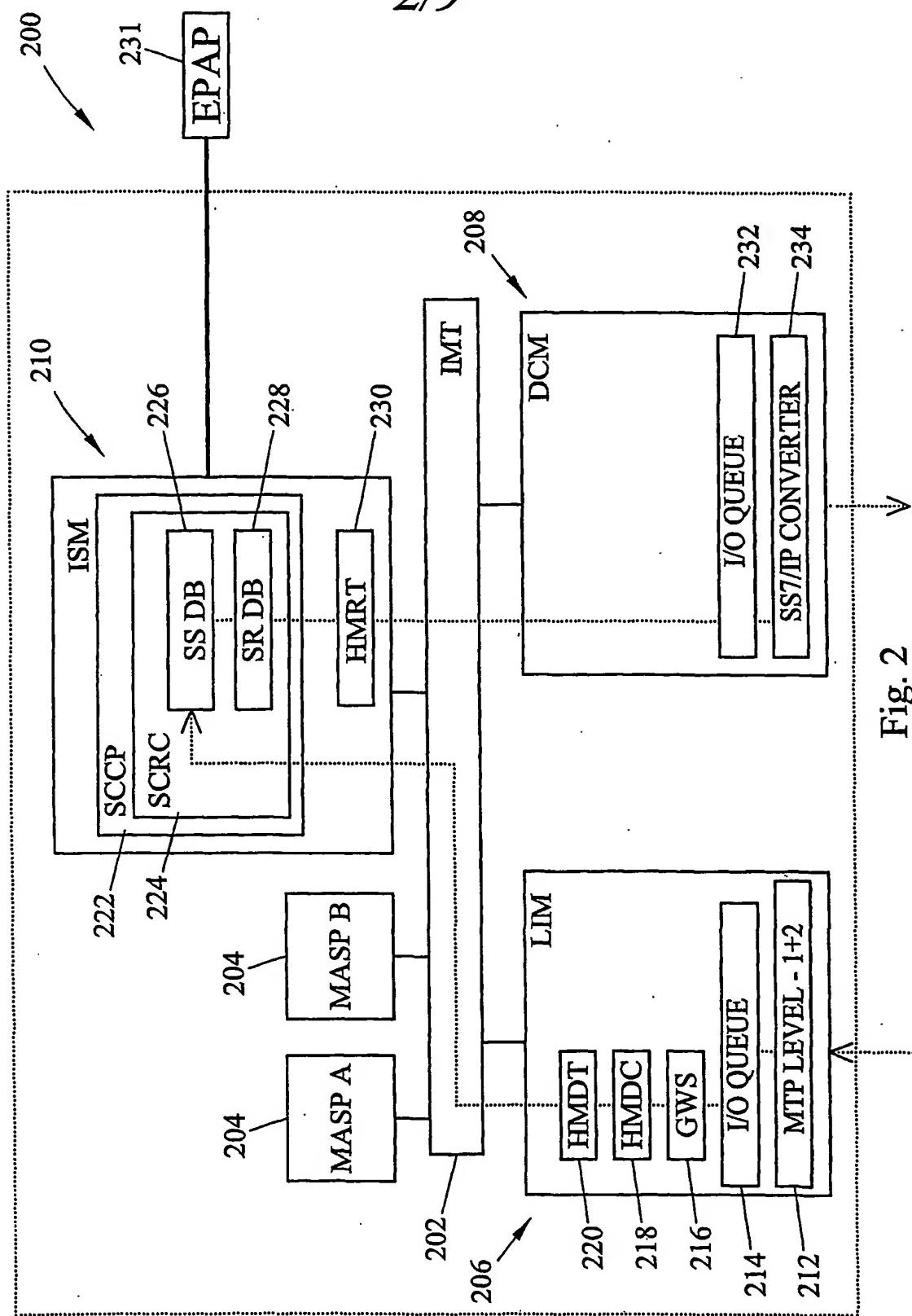


Fig. 2

3/9

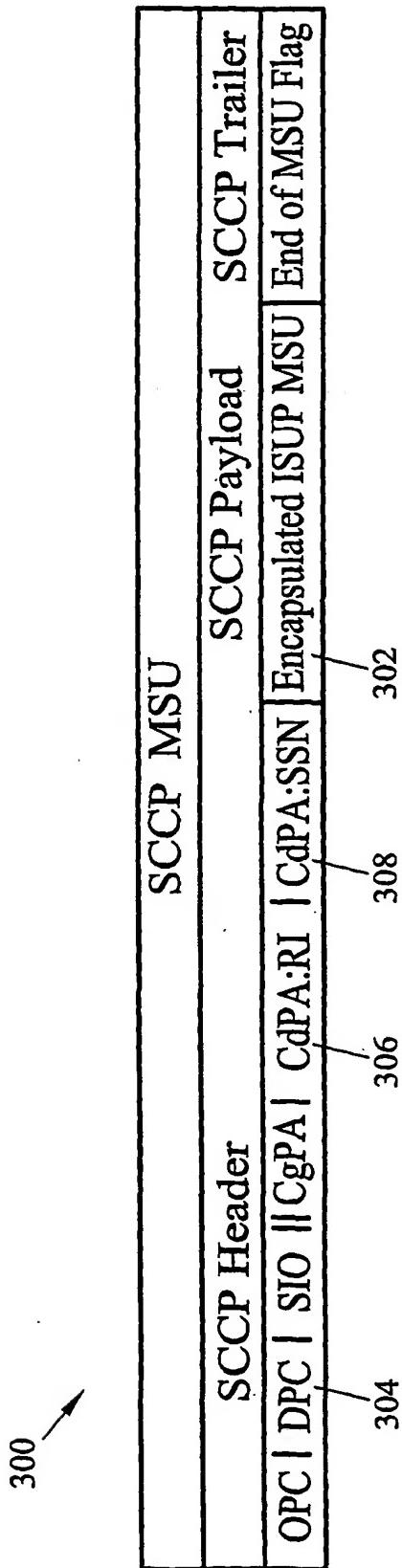


Fig. 3

4/9

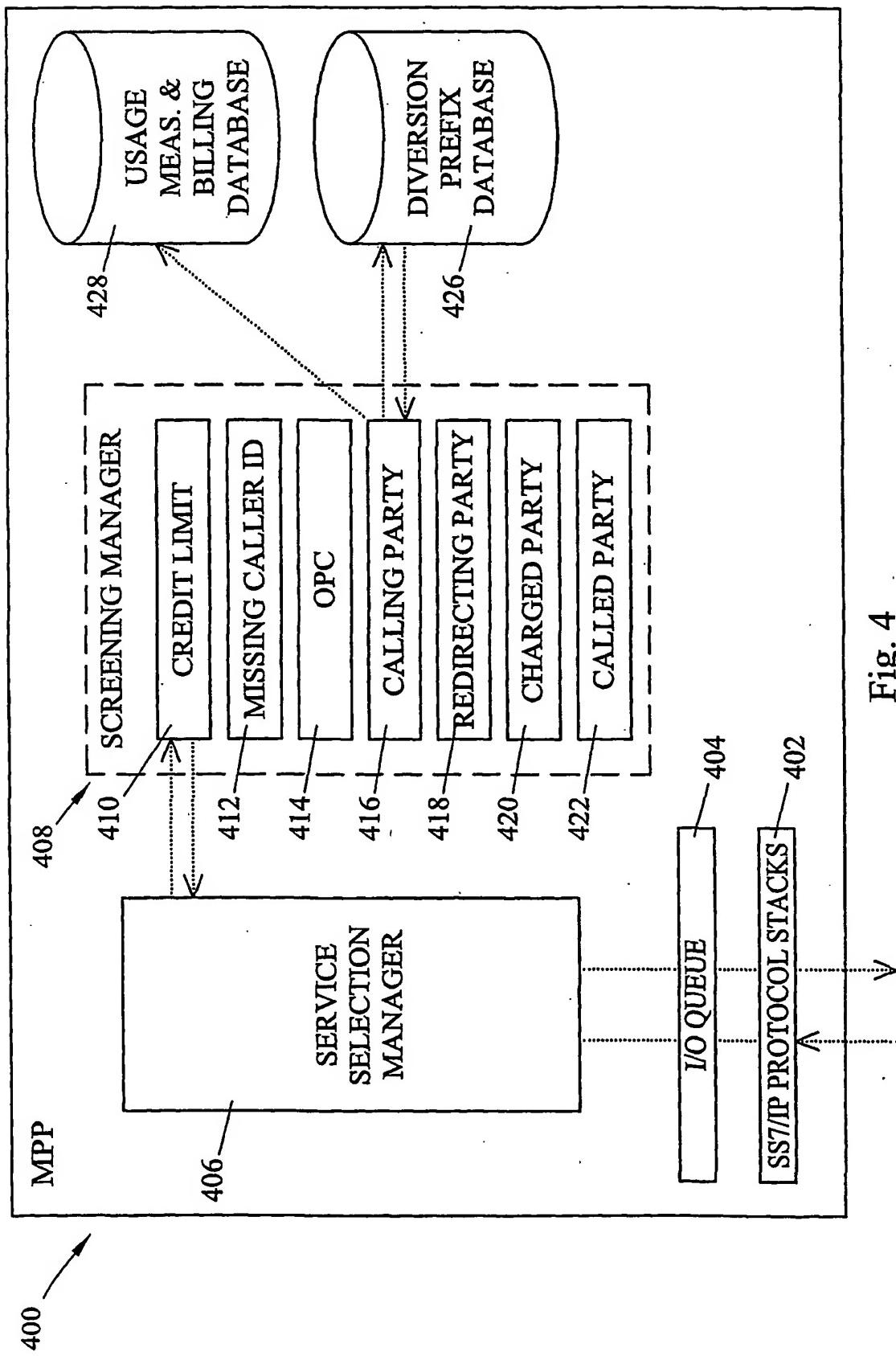


Fig. 4

5/9

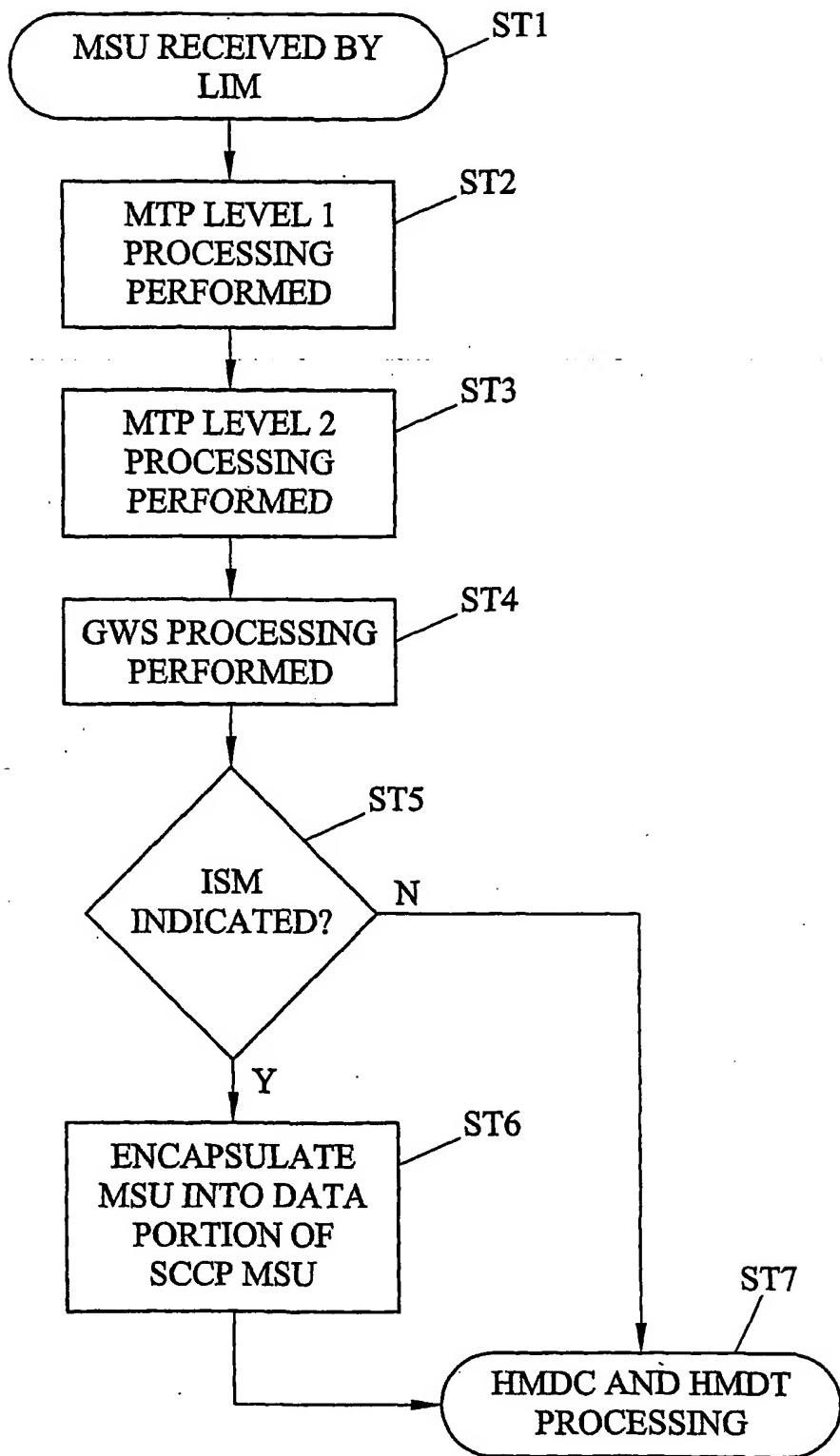


Fig. 5A

6/9

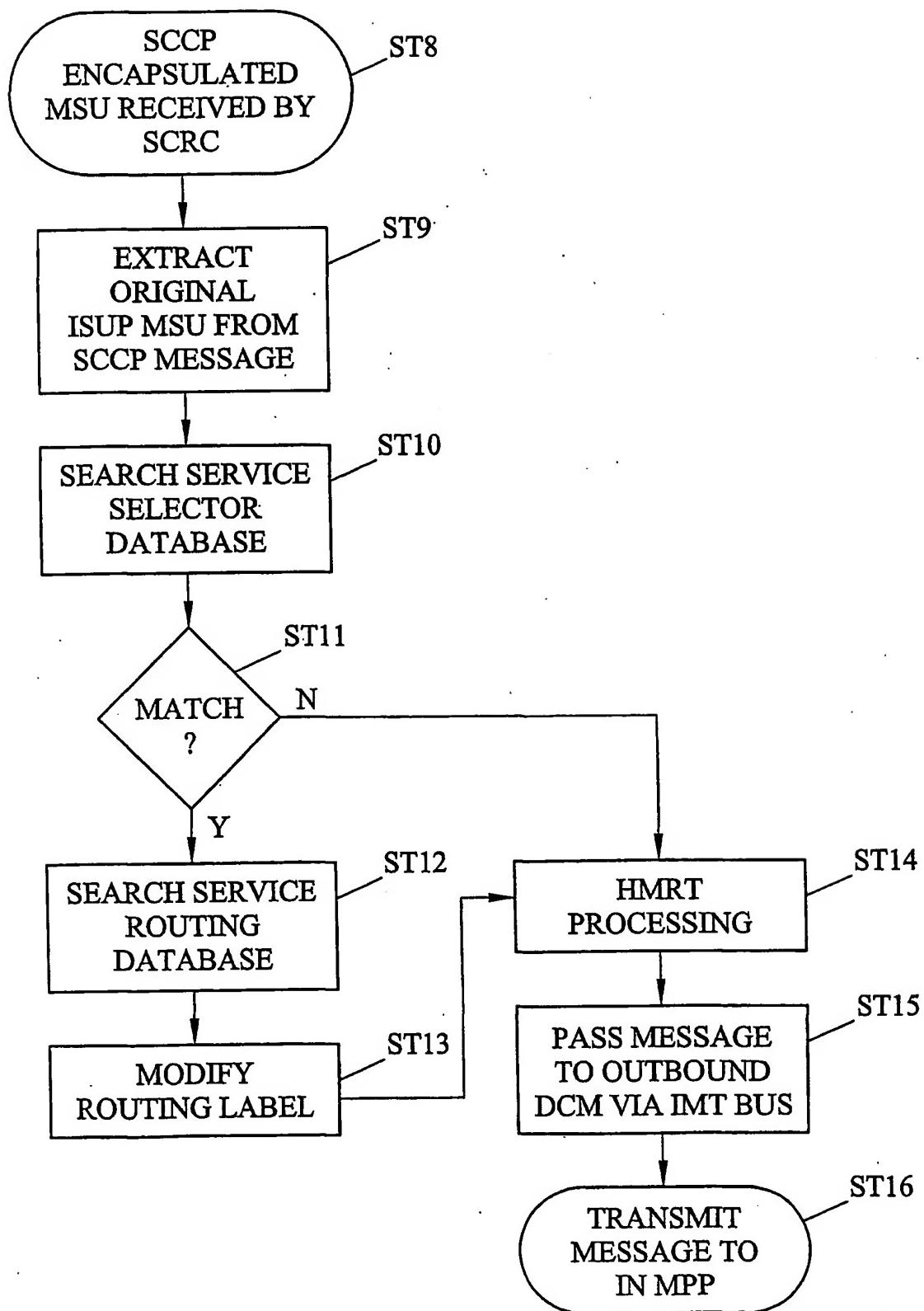


Fig. 5B

7/9

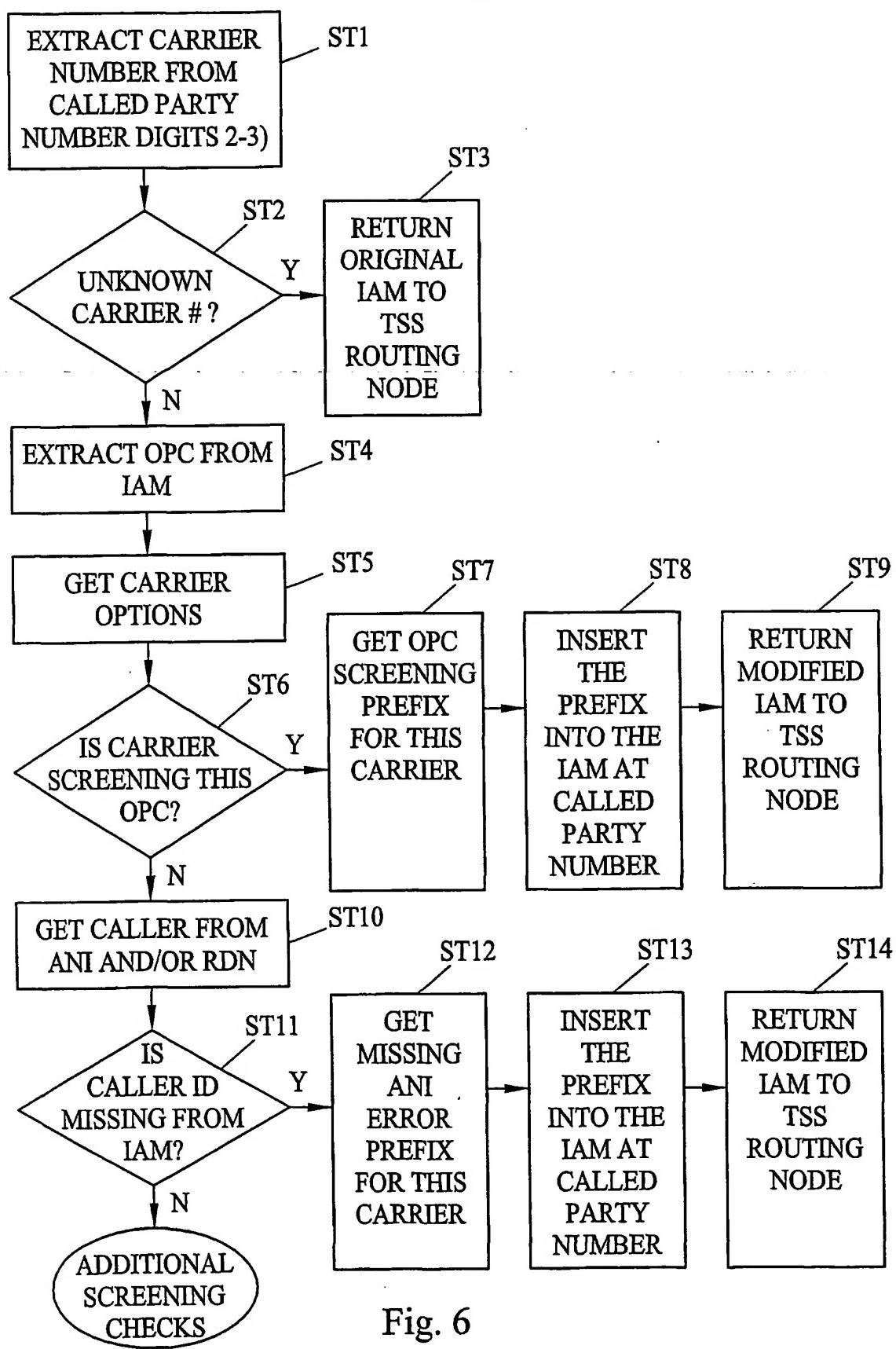


Fig. 6

8/9

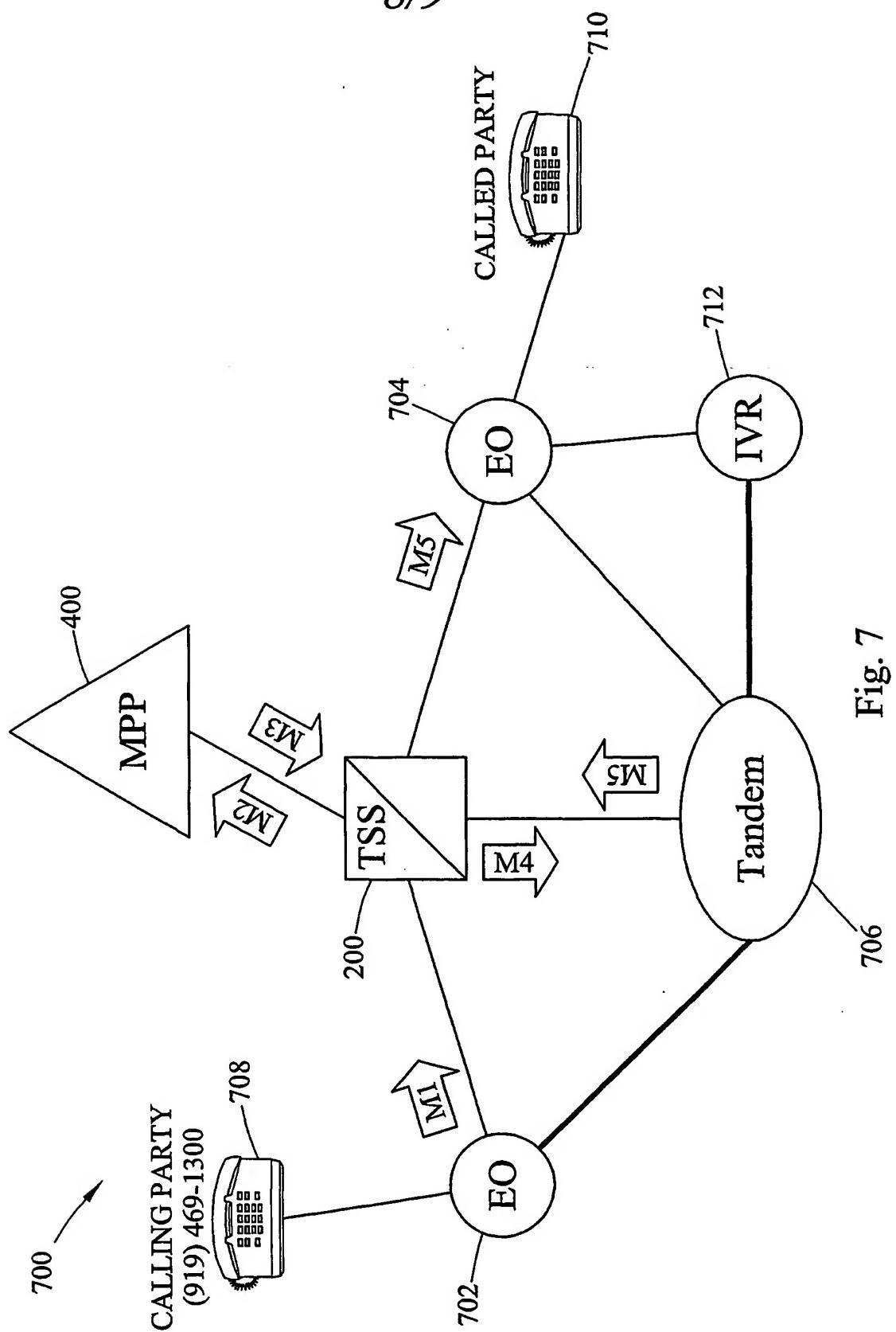


Fig. 7

9/9

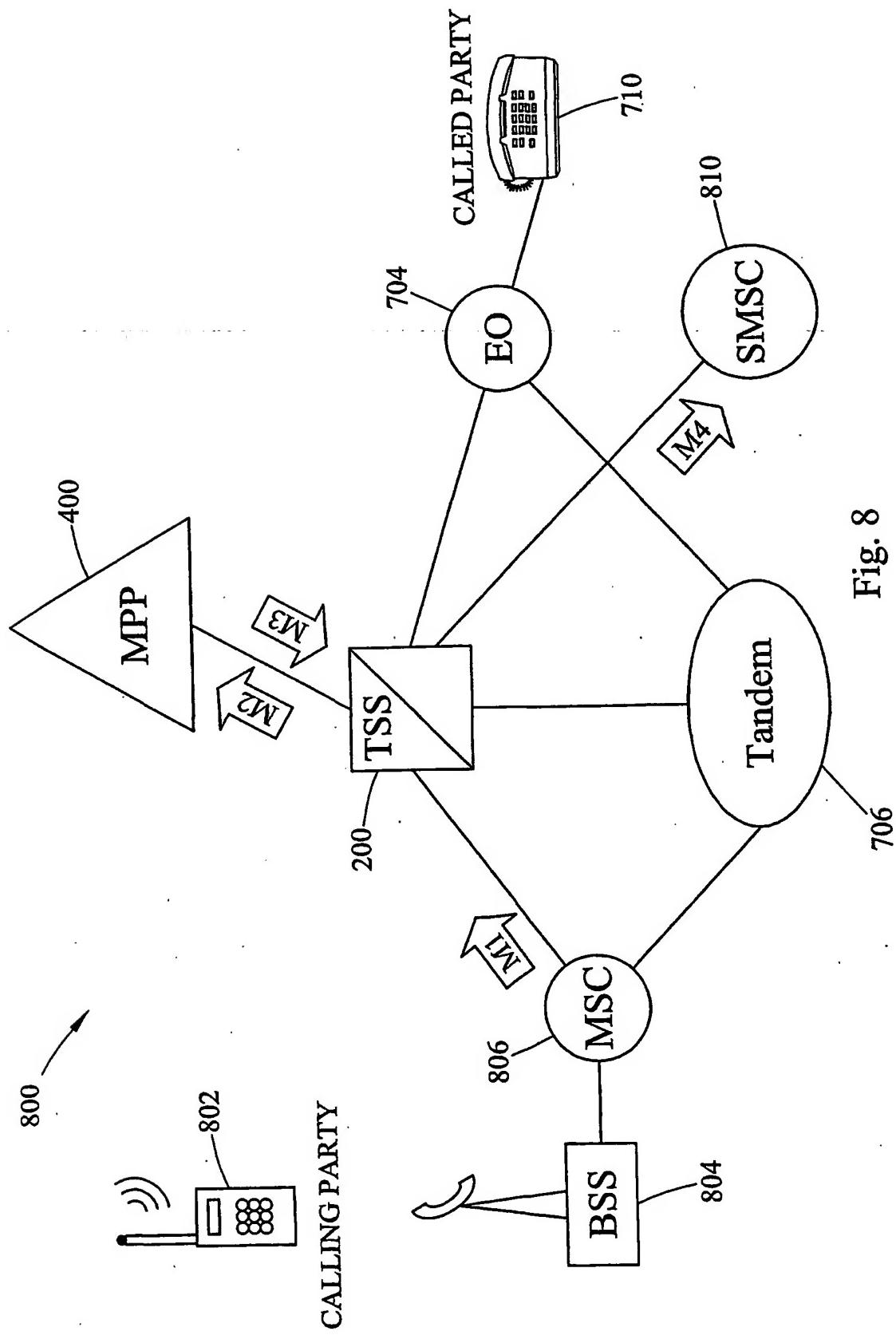


Fig. 8

## INTERNATIONAL SEARCH REPORT

Int'l Application No  
PCT/US 01/22093

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 H04Q3/00 H04M7/00 H04M3/436

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04Q H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DALGIC I ET AL: "TRUE NUMBER PORTABILITY AND ADVANCED CALL SCREENING IN A SIP-BASED IP TELEPHONY SYSTEM" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, N.J, US, vol. 37, no. 7, July 1999 (1999-07), pages 96-101, XP000835310 ISSN: 0163-6804 the whole document	1-47
A	US 5 796 806 A (BIRCKBICHLER RICH D) 18 August 1998 (1998-08-18) column 1, line 48 -column 2, line 4 column 3, line 19 - line 57 figure 2	1-47

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

## \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the International filing date but later than the priority date claimed

- "T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

23 November 2001

Date of mailing of the International search report

29/11/2001

## Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

## Authorized officer

Chassatte, R

**INTERNATIONAL SEARCH REPORT**International Application No  
PCT/US 01/22093

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5796806	A 18-08-1998	NONE	